O uso de ferramentas de segurança da informação para detectar ataques é bastante comum em ambientes especializados. As técnicas utilizadas são as mais variadas. A detecção de intrusão é vista como um processo de monitoramento de eventos que ocorre em um sistema de computador ou rede para detectar sinais de possíveis incidentes. Para tanto, tais técnicas utilizam ferramentas como os sistemas detectores de intrusão ou simplesmente IDS. Um problema conhecido dos IDS é que seu mecanismo de detecção requer o conhecimento prévio do ataque, normalmente embasado em critérios de assinaturas, que o identificam unicamente como um evento malicioso. Obviamente, a questão complementar de como coletar, analisar e visualizar os dados de tráfego que incluam possíveis ataques ainda desconhecidos, preferencialmente em tempo real, é um fator crítico e atual. A quantidade de ataques ainda desconhecidos perpetrados contra sistemas de computadores baseada em redes é muito grande. O uso de IDS é complementar ao uso de honeypots ou honeynets, que são técnicas utilizadas para serem deixadas em pontos específicos da rede, com a intenção explícita de serem atacadas, invadidas ou comprometidas. O ponto forte dessas técnicas está no fato de elas fazerem parte de uma solução de monitoramento, o que permite o descobrimento de novas formas de ataque. O uso de soluções que permitam a visualização em tempo real do ataque e as manobras realizadas pelo invasor também é desejável. Por meio de tais técnicas, analistas de segurança e especialistas em redes podem acompanhar os desdobramentos de um ataque e os passos que foram utilizados por um atacante para o comprometimento do sistema-alvo. Mediante tais observações, os analistas e especialistas em segurança podem criar novas assinaturas e atualizar o IDS, de forma que este seja capaz de detectar ataques desconhecidos. Contudo, o problema é que o IDS não bloqueia o ataque, mas registra que houve um. Assim, outras soluções devem ser utilizadas em conjunto.